云安全中心

产品简介

腾讯云

【版权声明】

【商标声明】

【服务声明】

本文档意在向您介绍腾讯云全部或部分产品、服务的当时的相关概况，部分产品、服务的内容可能不时有所调整。您所购买的腾讯云产品、服务的种类、服务标准等应由您与腾讯云之间的商业合同约定，除非双方另有约定，否则，腾讯云对本文档内容不做任何明示或默示的承诺或保证。

【联系我们】

我们致力于为您提供个性化的售前购买咨询服务，及相应的技术售后服务，任何问题请联系 4009100100或95716。

文档目录

产品简介
产品概述

最近更新时间：2026-04-30 14:08:12

云安全中心（Cloud Security Center，CSC）是腾讯云面向公有云用户推出的新一代云原生安全平台，以“**预防 → 检测 → 响应**”安全生命周期为核心框架，将主机安全、容器安全、云安全态势、AI 资产保护、数据安全等能力统一纳管，帮助企业构建从资产摸底到威胁闭环的一体化云上安全体系。

核心理念

云安全中心基于以下四项核心设计逻辑构建：

设计逻辑	含义
统一资产基座	主机、容器、AI 资产、云产品等资产统一管理，减少资产孤岛。
安全左移	将漏洞、基线、合规纳入事前治理，在风险演变为攻击前主动修复。
运行时防护	实时检测入侵、勒索等攻击行为，识别拦截正在发生的威胁。
运营闭环	以主动运营与智能配置为核心，结合 AI Copilot 提升处置效率。

核心能力

1. 概览

安全决策的统一入口。以安全分指标直观呈现安全健康度，通过**待办任务**引导您快速处理高优先级安全风险，让管理者一眼掌握云上整体安全态势。

2. AI 工作台

内置于云安全中心全流程的智能安全助手，支持：

- 自然语言查询安全事件、资产风险与漏洞详情分析。
- 辅助分析告警、生成处置建议与操作指引。
- 作为安全运营的核心智能引擎，降低人工运营成本。

3. 资产中心

摸清家底，是做好云安全的第一步。 资产中心提供统一的全景资产视图：

资产类型	说明
主机资产	云上服务器（CVM/轻量云/黑石等）统一纳管。

云资产	云数据库、存储桶、负载均衡等云产品资产统一梳理。

4. 风险治理（事前预防）

解决“如果不修，可能出事”的问题，实现风险的主动发现与闭环修复。

功能模块	核心能力
漏洞治理	检测操作系统及应用组件漏洞，支持优先级排序与一键修复。
云安全态势管理	云产品配置合规检查、系统基线治理、云边界暴露面分析。
AI Agent 安全	面向 AI 智能体的专项风险识别与防护。
云 API 风险治理	发现 API 暴露面风险、鉴权缺失及敏感数据泄露。
数据安全态势	梳理数据资产分布，识别数据安全风险与合规缺口。

5. 检测响应（事中防护）

解决“正在发生的攻击”问题，支持高效的实时检测与原始日志联动分析。

功能模块	核心能力
告警中心	汇聚主机入侵、容器入侵、API Server 日志异常等全类型安全告警，支持统一研判与一键处置。

6. 安全运营（事后溯源）

提供原始证据，支持自定义报表与深度审计，AI Copilot 是安全运营的核心亮点。

功能模块	核心能力
日志分析	对主机、容器等多类型日志进行深度搜索与分析，支持溯源。

7. 防护配置（主动运营）

统一管理各类防护策略，低频但关键的配置中心。

主机防护

- **勒索检测**：实时识别勒索软件行为，识别并阻断恶意进程。
- **核心文件监控**：防止关键系统文件与 Web 页面被恶意篡改。

应用防护

- 针对 Web 应用与 API 的应用层安全防护配置。

8. 系统设置

统一接入入口，便于您进行系统配置的管理。

功能模块	说明
通知中心	安全告警、风险变化的多渠道通知配置。
接入管理	Agent 客户端安装与多云、多账户统一接入管理。
授权管理	产品功能授权与许可证统一管理。

覆盖的安全场景

表中列出的安全场景仅为部分示例。

安全场景	描述	涉及功能模块
云上资产统一可见	主机、容器、AI 资产、云产品资产全面纳管，建立动态安全台账。	资产中心
漏洞与基线合规治理	事前发现系统漏洞、错误配置与合规缺口，主动修复。	风险治理（漏洞、CSPM）
AI 与新兴资产安全	覆盖 AI Agent、AI 推理服务等新型资产的专项安全防护。	风险治理（AI Agent）、资产中心
数据安全与隐私合规	数据资产梳理、敏感数据发现、数据风险态势管理。	风险治理（DSPM）、快照检测
实时入侵检测与响应	主机、容器、API 入侵的实时告警与联动处置。	检测响应（告警中心）
勒索防护	勒索软件行为实时检测与阻断，核心文件防篡改。	防护配置（主机防护）
安全合规与审计	等保 2.0 合规检查、安全审计报告、日志留存溯源。	安全运营（报告、日志分析）、CSPM
多云统一安全管理	跨云账户、跨云平台的资产与安全策略的统一管理。	系统设置（多云接入）、资产中心

适用人群

用户角色	使用场景
云上安全负责人 / CISO	通过概览掌握企业安全健康度，驱动安全治理决策制定。

安全运营工程师	每日处置告警、修复漏洞、跟进风险治理闭环工作。
DevOps / 开发工程师	接入 CI/CD 安全扫描、IaC 检测，实现安全研发左移的目标。
合规审计人员	获取等保 2.0 合规报告、安全审计日志与证明材料。
容器 / 云原生工程师	管理集群安全配置、镜像风险与容器运行时防护策略。

热点问题（FAQ）

Q：云安全中心支持哪些类型的云资产接入?

A：支持主机（CVM）、Kubernetes 容器集群以及云数据库、对象存储、负载均衡等腾讯云产品资产的统一接入与管理。

Q：产品如何支持多云或多账户场景?

A：通过「系统设置 → 接入管理」实现多云平台、多腾讯云账户的统一接入，并在资产中心统一展示跨账户的资产与风险态势。

Q：如何快速开展漏洞治理工作?

A：进入「风险治理 → 漏洞治理」，系统将自动展示资产漏洞列表及修复优先级建议，支持一键下发修复任务指令（该操作可能导致服务中断或数据丢失，建议按照产品指南创建快照，实现快速恢复能力）。

Q：如何帮助企业满足等保 2.0 要求?

A：「风险治理 → 云安全态势管理」内置等保 2.0 合规基线检测项，「安全运营 → 日志分析」支持日志存储180天，进行安全审计和溯源。

Q：AI Copilot 在哪些场景下能提升效率?

A：AI Copilot 贯穿产品全流程，典型场景包括：通过自然语言查询告警详情与处置建议、辅助分析威胁日志、快速生成安全报告摘要。

Q：如何开始使用云安全中心?

A：登录腾讯云控制台，搜索“云安全中心”即可进入产品。建议首先通过「系统设置 → 接入管理」完成 Agent 安装和资产接入，再进入「资产中心」完成资产梳理，随后依据「概览」页面的待办事项逐步推进风险治理工作进程。

产品优势

最近更新时间：2026-04-30 14:08:12

综合对比总览

对比维度	传统单点安全产品	云安全中心
管理方式	多控制台分散管理	统一平台集中管理
资产覆盖	以主机/网络为主	主机+容器+ AI 资产+云产品全覆盖
防护阶段	单一阶段，覆盖有限	预防、检测、响应全生命周期
AI 能力	无或基础规则引擎	AI Copilot 贯穿全流程
安全左移	不支持	CI/CD、IaC、镜像安全
部署复杂度	多产品独立部署维护	云原生 SaaS，轻量 Agent
合规支持	跨系统举证，效率低	一键合规检查
运营门槛	依赖大量专业人力	AI 辅助，降低运营成本
事件关联	跨产品关联分析缺失	统一告警中心
新型资产	覆盖能力有限	AI 资产、K8s 原生支持

优势一：统一平台，打破安全孤岛

传统单点产品的问题

企业通常采购多款独立安全产品，各产品分别部署、独立管理，数据互不互通。安全团队需要在多个控制台之间频繁切换，资产、事件、策略无法形成关联，形成大量安全孤岛，整体安全态势不可见。

云安全中心的做法

以**统一资产基座**为核心，将主机、容器、AI 资产、云产品统一纳入同一平台管理，一个控制台即可掌握全网资产的安全状态。无论是漏洞、告警还是基线问题，均在同一平台中聚合呈现，消除安全孤岛。

对比维度	传统单点产品	腾讯云安全中心 CNAPP
控制台数量	多个产品各自独立控制台	统一控制台
资产管理	分散、碎片化	主机/容器/AI/云产品统一纳管
安全态势	无全局视图	统一安全健康度评分

策略管理	各产品独立配置	统一防护配置中心

优势二：全生命周期覆盖，构建纵深防御

传统单点产品的问题

单点产品通常只覆盖安全链条的某一环节，例如防火墙只做边界防护、漏洞扫描只做事前检测，缺乏从"预防到响应"的完整覆盖，攻击一旦穿透某一层防线即可长驱直入。

云安全中心的做法

以"**预防 → 检测 → 响应**"安全生命周期为核心框架，三个阶段衔接：

事前预防（风险治理）
└── 漏洞治理 / 云安全态势 / 合规基线 / 镜像风险 / 数据安全态势
↓
事中检测（检测响应）
└── 告警中心（主机入侵检测 / 容器入侵检测 / APIServer 异常检测等）
↓
事后溯源（安全运营）
└── 日志分析

单点产品只能解决其中一个阶段的问题，而腾讯云安全中心让三个阶段形成完整闭环。

优势三：AI Copilot 驱动，降低运营成本

传统单点产品的问题

传统安全产品产生大量告警，人工研判效率低，误报率高。安全运营往往需要资深工程师才能处置，中小团队难以承受高昂的人力成本，大量告警积压无人处理。

云安全中心的做法

内置 **AI Copilot 智能安全助手**，以大模型能力贯穿运营全流程：

- **告警智能研判**：分析告警上下文，区分真实威胁与误报，输出处置建议供参考。
- **自然语言查询**：支持用自然语言检索资产信息、事件详情，无需熟悉复杂查询语法。
- **威胁溯源辅助**：在日志分析与威胁狩猎中，AI 辅助还原攻击链，降低人工溯源难度。
- **报告智能生成**：自动归纳安全周期事件，生成可读性强的合规与运营报告。

对比维度	传统单点产品	腾讯云安全中心 CNAPP
告警处理	全量人工研判，效率低	AI 自动研判 + 处置建议

运营门槛	依赖资深安全工程师	AI Copilot 降低使用门槛
事件溯源	人工跨系统查日志	AI 辅助一键关联溯源
报告生成	手动整理，耗时费力	自动生成合规与运营报告

优势四：安全左移，将风险消灭在萌芽阶段

传统单点产品的问题

传统安全工具多以"亡羊补牢"为主，事件发生后才能检测响应。研发交付的镜像、代码、基础设施配置中存在的安全风险，往往在上线后才被发现，修复代价极高。

云安全中心的做法

将安全能力向研发侧前置，实现真正的研发安全运营（DevSecOps）：

- **容器镜像扫描**：在镜像入库和部署前检测漏洞、恶意样本与敏感数据。
- **CI/CD 流水线集成**：将安全检测内嵌到研发构建流程，代码提交即触发安全扫描。
- **IaC 安全检查**：对 IaC 等基础设施代码进行安全扫描，防止错误配置带入生产。
- **快照离线检测**：对云主机快照进行漏洞、基线检查与敏感数据检测，实现不影响业务的离线评估。

传统工具只能在运行态发现问题，腾讯云安全中心在**代码、镜像、配置**阶段即可介入，降低修复成本。

优势五：云原生深度集成，开箱即用

传统单点产品的问题

传统安全产品多为"搬迁上云"的架构，与云基础设施耦合度低（或耦合度不高），需要繁琐的手动配置资产、维护 agent 版本、对接云 API，运维复杂度高。新增资产往往不能自动纳管，存在资产盲区。

云安全中心的做法

作为**腾讯云原生产品**，与云基础设施深度集成，具体包括：

- **资产自动同步**：新增/释放云资源自动感知，资产台账实时更新。
- **多云统一接入**：通过系统设置中的接入管理，一键即可完成多云账户与资产的统一纳管。
- **无硬件依赖**：主机安全通过轻量 agent 部署，其余能力均为 SaaS 化服务，无需额外采购硬件。
- **联动响应**：与腾讯云 VPC、CVM、TKE、安全组等产品深度联动，实现告警到处置的自动化闭环。

优势六：覆盖新兴资产，应对 AI 时代安全威胁

传统单点产品的问题

传统安全产品的设计以 VM 和 Web 应用为核心，对容器、Kubernetes、AI Agent、大模型推理服务等新型云原生资产缺乏原生支持，防护存在大量空白区域。

云安全中心的做法

在传统资产防护基础上，率先覆盖 **AI 时代的新型资产安全**：

新兴资产类型	覆盖能力
AI 资产	AI Agent、推理服务的专项资产可见性与风险识别
AI Agent 安全	针对 AI 智能体的专项风险治理能力模块
容器与 K8s	镜像 → 集群 → 运行时环境 → 全链路防护
云 API	API 暴露面识别、鉴权风险检测与敏感数据泄露检测
数据安全	数据资产梳理与数据安全态势（DSPM）管理

优势七：合规检查开箱即用

传统单点产品的问题

等保合规、行业监管要求横跨网络、主机、数据等多个安全领域，使用单点产品时需要跨多系统分别举证，合规审查耗时费力，且难以形成完整的证据链。

云安全中心的做法

统一纳管各安全领域，内置合规检查基线与审计能力：

- **等保 2.0 合规基线**：覆盖主机配置、网络访问控制、漏洞管理等核心检查项。
- **云产品安全配置检查**：通过 CSPM 模块自动检测云产品错误配置与合规缺口问题。
- **完整日志留存**：主机、容器等全类型日志统一留存，支持监管要求的日志审计与溯源。

安全生命周期框架

最近更新时间：2026-04-30 14:08:12

云安全中心以安全生命周期为轴，构建“预防 — 检测 — 响应”三位一体的安全框架：

阶段	核心理念	解决的问题
事前风险治理	安全左移，主动发现并修复风险	“如果不改，可能出事”
事中检测响应	实时感知，进行阻断攻击	“正在发生的攻击怎么办”
事后安全运营	深度溯源，持续提升运营能力	“攻击发生后如何复盘与改进”

事前风险治理

核心目标：在风险演变为攻击之前，主动发现漏洞、错误配置与合规缺口，实现风险的闭环修复。

主机漏洞治理

对云上主机（服务器）进行全面的漏洞检测与修复管理：

- **漏洞自动检测**：持续扫描操作系统及应用组件漏洞，覆盖 CVE、CNVD 等主流漏洞库。
- **风险优先级排序**：结合资产重要性与漏洞威胁等级，输出高优先级修复建议。
- **修复任务闭环**：支持一键下发修复任务，跟踪修复进度至闭环。

云安全态势管理

全面检查云上产品配置安全与合规状态：

- **云产品配置检查**：自动检测云数据库、存储桶、网络安全组等云产品的错误配置。
- **系统基线治理**：内置等保 2.0、CIS 等主流安全基线，发现主机系统配置风险。
- **云边界分析**：梳理互联网暴露面，识别不必要的端口开放与访问控制缺失。

快照检测

对云主机快照进行离线安全评估，不影响业务运行：

- 支持快照中漏洞的全面检测。
- 适用于主机备份的安全合规核查场景。

云 API 风险治理

发现云 API 层面的安全隐患：

- **API 暴露面识别**：梳理对外暴露的 API 接口，识别未授权访问风险。
- **鉴权风险检测**：发现 API 鉴权缺失、权限过大等配置问题。
- **敏感数据泄露检测**：检测 API 响应中存在的敏感信息外泄风险。

AI Agent 安全

面向 AI 智能体的专项安全风险识别与防护：

- 识别 AI Agent 运行过程中的异常行为与安全风险。
- 管理 AI Agent 资产，构建 AI 业务的安全可见性。

数据安全态势

梳理数据资产分布，管理数据安全风险：

- **数据资产发现**：自动识别云上数据库、存储桶中的敏感数据分布。
- **数据风险评估**：识别数据访问权限过大、数据泄露等安全风险。
- **合规缺口分析**：对照数据安全相关法规，输出合规缺口建议。

事中检测响应

核心目标：实时感知主机、容器、网络、API 层的入侵与攻击行为，支持快速研判与联动处置。

告警中心

汇聚全类型安全告警的统一研判与处置平台：

覆盖告警类型

告警类型	具体场景
主机入侵告警	恶意进程、暴力破解、异常登录、木马植入、反弹 Shell、异常命令等
勒索行为告警	勒索软件行为识别、文件加密行为阻断

核心能力

- **AI 辅助研判**：AI Copilot 自动分析告警上下文，区分真实威胁与误报，输出处置建议。
- **一键处置**：支持告警确认、隔离、封禁等一键响应操作。
- **告警关联**：自动关联同一攻击链的多条告警，还原攻击全貌。

事后安全运营

核心目标：提供完整的日志留存与审计能力，支持事件复盘、合规证明与持续运营改进。

日志分析

对多类型安全日志进行深度搜索与分析：

- **多源日志采集**：统一采集主机日志（进程、网络、文件）、容器日志、云产品访问日志。
- **全文检索**：支持按时间、主机、IP、关键字等多维度快速检索日志。
- **溯源取证**：还原攻击入侵路径，生成可作为证明材料的完整日志链。

应用场景

最近更新时间：2026-04-30 14:08:12

本文档以安全场景为视角，介绍典型工作场景下云安全中心产品提供的价值，帮助您快速找到与自身需求相关的产品功能。

安全场景	产品价值
云上资产底数不清 资产分散多账户，数量不清、风险不明，安全工作无从下手。	• 资产中心统一纳管主机、容器、云产品，自动同步变更； • 概览以安全健康评分量化风险水位，让“资产不清、风险不明”变为一图可见、优先级一目了然。
漏洞修复周期长 扫描结果堆积，不知修哪个最急；手动逐台修复，效率极低。	• 综合 CVSS 评分与资产重要性等维度自动输出修复优先级； • Linux / Windows / Web-CMS 漏洞支持一键批量修复，显著压缩高危漏洞暴露窗口。
云产品配置错误，敏感数据面临泄露 存储桶公开可读、安全组过度放开等配置错误静默存在，是数据泄露的直接根因。	• CSPM 自动扫描云数据库、存储桶、安全组等错误配置；DSPM 识别敏感数据暴露风险； • 云边界分析量化攻击面——从靠运气发现变为持续自动扫描、风险主动暴露。
等保合规举证耗时费力 每次评审需手动收集漏洞、日志、配置等材料，费时且易遗漏。	• 内置等保二级/三级、CIS Benchmark 基线，自动扫描并输出整改建议； • 一键检查——让合规从“临时突击”变为日常持续、随时可证。
入侵告警处置效率低 海量告警误报混杂，人工研判耗时；跨工具处置响应链路长。	• AI Copilot 自动区分真实威胁与误报并输出处置建议，研判时间从分钟级压缩至秒级； • 同攻击链告警自动聚合；主机隔离、IP 封禁等操作单页面一键执行，提升响应效率。
勒索软件威胁，业务面临瘫痪风险 文件被批量加密、业务数分钟内瘫痪，传统工具感知严重滞后。	• 实时监控进程行为，在扩散前识别勒索特征并触发告警，支持一键网络隔离阻断横向传播； • 快照检测确认备份数据未被感染，保障业务快速安全恢复。
容器集群遭受攻击，云原生安全可见性差 容器逃逸、K8s 横向移动等攻击传统工具无法覆盖，入侵痕迹难以追溯。	• 容器运行时威胁检测实时感知容器逃逸与异常进程；K8s APIServer 日志监控识别集群控制层高危操作；

安全检测缺失，漏洞随镜像带入生产 镜像漏洞、硬编码密钥在生产运行数周后才被发现，修复成本极高。	• CI/CD 集成在构建阶段自动扫描，高危漏洞自动阻断发布；镜像仓库持续扫描漏洞与敏感凭据； • IaC 扫描在代码提交阶段发现配置风险——将安全检测从上线后补救左移至构建阶段拦截。
安全事件溯源困难，无法快速还原攻击全貌 日志分散多处，人工检索耗时数天；事后难以出具完整事件报告。	• 日志分析统一采集主机、容器、K8s 审计日志，支持全文检索； • AI Copilot 自然语言溯源，将分析时间从数小时压缩至分钟级； • 自动还原攻击链，可提交管理层。
安全投入难量化，管理层无法评估成效 安全工作被视为黑盒成本，无数据支撑。	• 安全健康评分持续量化全网安全水位；漏洞修复量、合规率、告警处置率等指标全程记录； • 将安全工作从“无法量化的黑盒”变为有据可查的可视化资产。

版本与适用场景

最近更新时间：2026-04-30 14:08:12

功能集定位速览

功能集	核心定位	价格	适合企业类型
主机安全 · 专业版	主机基础安全加固	80元/台/月	以云服务器为主、需基础防护的中小企业
主机安全 · 旗舰版	主机安全完整防护 + 合规	180元/台/月	有等保合规要求的中大型企业

以下模块在所有付费版本均可单独叠加采购，不受版本限制：

模块	核心价值	建议搭配场景
云产品配置检查	检查数据库、存储桶、安全组等云产品错误配置	云产品种类多、配置风险高的企业
数据安全态势	梳理敏感数据分布、数据合规风险	有数据安全法/个人信息保护法合规要求的企业
日志分析	原始日志留存、深度检索与合规审计	有等保日志留存要求或需深度溯源的企业
应用防护	Web 应用层安全防护	有强安全对抗的场景，应用层保护的企业业务
云 API 风险治理	API 暴露面管理、鉴权风险深度检测	API 数量多、服务复杂的企业

版本功能对比全览

功能模块	免费版	主机安全（专业版）	主机安全（旗舰版）
资产中心（主机/容器/云资产）	✓	✓	✓
应急漏洞检测	✓	✓	✓
告警中心（异地登录）	✓	✓	✓
AI Copilot	×	✓	✓
Linux/Windows/Web-CMS 漏洞一键修复	×	✓	✓

弱口令基线检测	×	✓	✓
告警中心（防病毒）	×	✓	✓
漏洞虚拟补丁	×	×	✓
应用漏洞检测	×	×	✓
等保 2.0 / CIS 等合规基线	×	×	✓
云边界分析	×	×	✓
AI Agent 安全	×	×	✓
勒索检测	×	×	✓
核心文件监控	×	×	✓
告警中心（主机高级威胁检测）	×	×	✓
云产品配置检查	×	按需采购	按需采购
数据安全态势	×	按需采购	按需采购
日志分析	×	按需采购	按需采购
应用防护	×	按需采购	按需采购
云 API 风险治理	×	按需采购	按需采购

各版本详解

主机安全（专业版）

适合企业特征

- 云上资产以**云服务器为主**。
- 曾遭遇暴力破解、木马、异常登录等基础入侵威胁。
- 处于安全建设初期，需以合理成本建立核心主机防护基线。
- **无**等保合规要求，或仅需基础弱口令管理。

相比免费版新增的核心能力

能力项	具体说明
漏洞一键修复	Linux / Windows / Web-CMS 漏洞均支持一键修复

应用漏洞检测	系统服务弱口令、应用服务漏洞全面检测
弱口令基线	自动发现系统弱口令配置风险
告警中心（防病毒）	接收恶意样本、主机入侵、异常登录、恶意进程等核心告警
AI Copilot	AI 辅助告警研判，自动输出处置建议

仍然缺失的能力

- 无等保 2.0 / CIS 合规基线检测。
- 无云边界暴露面分析。
- 高级威胁检测能力不包含（APT 等复杂攻击无法识别）。
- 无核心文件监控，关键文件被篡改无感知。

典型场景：某电商企业有 30 台云服务器，曾遭受 SSH 暴力破解，选择专业版后开启漏洞一键修复、弱口令检测和入侵告警，以合理成本完成主机防护基线建设。

主机安全（旗舰版）

适合企业特征

- 有明确的**等保 2.0 合规要求**（二级或三级）检查项。
- 资产规模较大（50 台服务器以上），安全暴露面广。
- 有专职安全团队，需要完整的威胁检测与响应能力。
- 遭遇过 APT 等高级攻击，或所处行业安全风险较高。

相比专业版新增的核心能力

能力项	具体说明
等保 / CIS 合规基线	内置等保二级/三级、CIS Benchmark、腾讯云基线标准，支持一键合规检测
云边界分析	梳理互联网暴露面，识别不必要的端口开放与访问控制缺失
高级威胁检测	告警中心升级，覆盖 APT 等复杂攻击模式
核心文件监控	关键系统文件与 Web 页面防篡改实时监控
AI Agent 安全	覆盖 AI 智能体资产的安全管理与风险识别

典型场景一（合规驱动）：某医疗企业需每年通过等保三级评审，旗舰版内置等保基线检测，降低评审准备工作量。
典型场景二（高级威胁）：某企业安全团队发现可疑进程但告警中心无记录，通过日志分析基于原始日志主动排查，成功发现绕过规则检测的隐蔽 APT 攻击行为。

热点问题

Q：免费版什么时候升级?

A：出现以下任一情况建议立即升级：① 遭遇暴力破解或入侵事件；② 有勒索防护或文件监控需求；③ 有漏洞需要快速修复；④ 有等保合规要求；

Q：按需采购如何选择最适合的模块?

A：根据实际业务痛点按需叠加：

- 有等保日志留存要求 → 叠加**日志分析**；
- 云产品种类多配置风险大 → 叠加**云产品配置检查**；
- 有数据安全合规要求 → 叠加**DSPM**；
- 有强安全攻防对抗 → 叠加**应用防护**；
- 无法安装客户端进行防护需求 → 叠加**快照检测**。